International Journal of Science Engineering and Advance Technology

# Cloud Assisted Mobile Access of Health Data With Privacy and Audit Ability

Navuduri Sruthi [1], K.Lakshmi Priya [2]
[1]PG Scholar, Pydah College of Engineering, Kakinada, AP, India, E-mail: sruthi.it41@gmail.com.
[2]Assistant Professor, Pydah College of Engineering, Kakinada, AP, India.

Abstract— Monitoring and advising patients via mobile health care system is the current trend in medical field that acts as a life saver due to its availability at anytime and anywhere. This e-healthcare system requires patient's private data to be available at cloud, outsourced data storage. This situation faces privacy issues. Hence the proposed approach focus on providing a private cloud for mobile users to ensure less cost, effective and secure storage. The data keyed in the mobile is transferred to private cloud, which in turn is processed and again transferred to public cloud. The sensitivity of the outsourced cloud data is maintained using Attribute based Encryption technique which restricts data access based on encrypt/decrypt of data with its access structures. The data privacy is ensured by PRF based key management and secures indexing methodologies. Personal Health records view ability access control to the actual data owner is the core idea of this project. The project segregates the access users in to Public Domain Users and Private Domain users.
Key words: e-Health, Privacy, Auditability, Access Control.

## I. INTRODUCTION

To facilitate our discussion, we first elaborate our cloudassisted mHealth monitoring system (CAM). CAM consists of four parties: the cloud server (simply the cloud), the company who provides the mHealth monitoring service (i.e., the healthcare service provider), the individual clients (simply clients), and a semi-trusted authority (TA). The company stores its encrypted monitoring data or program in the cloud server. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through a mobile (or smart) device. A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client input vectors. We assume a neutral cloud server, which means it neither colludes with the company nor a client to attack the other side.

## II. RELATED WORK

The survey contains various details about cloud security, methods of encryption and decryption techniques, several issues and parameters were considered. According to A Rule-Based Framework for Role-Based Delegation and Revocation studied by Longhua Zhang et al. [9] the protection of data privacy, sensitive data has to be Rule-Based Framework before outsourcing, which makes effective data utilization a very challenging task. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. Ranked searchable symmetric encryption gives an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE). But this approach suffers from two main drawbacks when directly applied in the context of Cloud Computing. The Rule-Based Framework cloud data have to post process every retrieved file in order to find ones most matching their interest; On the other hand, invariably retrieving all files containing the queried keyword further incurs unnecessary network traffic. HCPP - Healthcare system for Patient Privacy is based on cryptographic constructions and existing wireless network infrastructures studied by Jinyuan Sun et al. [3] specify the techniques that are provably secure. The techniques provide provable secrecy for encryption, in the sense that the untreated server cannot learn anything about the plaintext given only the cipher text. The techniques provide controlled searching, so that the non trusted server cannot search for a word without the user's authorization. But, the drawbacks are it searches encrypted data without an index .This performs normal searchable scan method using pseudorandom generator for search techniques. A Security Architecture for Computational Grids by Ian Foster et al. [10] says that for protecting data grid, sensitive data has to be encrypted before outsourcing of grid, which obsoletes traditional data utilization based on plaintext keyword search. There are large number of data grid and documents in cloud, it is crucial for the search service to allow multikeyword grid and provide result similarity ranking to meet the effective data retrieval need. The merits are Coordinate matching-as many matches as possible. Inner product similarity -The number of grid

keywords appearing in a document. The number of grid keywords appearing in the document to quantify the similarity of that document to the query. But this paper faces with these drawbacks. The Multi-keyword Ranked search algorithm provides multi keyword to search over cloud data provides numerous data results.

## III. SYSTEM ANALYSIS

### EXISTING SYSTEM:

Existing Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology.

### PROPOSED SYSTEM:

CAM consists of four parties: the cloud server (simply the cloud), the company who provides the mHealth monitoring service (i.e., the healthcare service provider), the individual clients (simply clients), and a semi-trusted authority (TA). The company stores its encrypted monitoring data or program in the cloud server. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through a mobile (or smart) device. A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client input vectors.

### Merits of the Proposed System:

The storage overhead is linear with the number of outsourced healthcare data files, while the communication overhead can be considered as constant per data request. The result indicates that the proposed scheme is efficient as well as scalable

## IV. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

### MODULE DESCRIPTION:

Branching Program:

we formally describe the branching programs, which include binary classification or decision trees as aspecial case. We only consider the binary branching program for the ease of exposition since a privatequery protocol based on a general decision tree can be easily derived from our scheme. Let v be the vector of clients' attributes. To be more specific, an attribute component *vi* is a concatenation of an attribute index and the respective attribute value. For instance, A||KW1 might correspond to "blood pressure: 130". Those with a blood pressure lower than 130 are considered as normal, and those above this threshold are considered as high blood pressure. The first element is a set of nodes in the branching tree. The non-leaf node p*i* is an intermediate decision node while leaf node p*i* is a label node. Each decision node is a pair (*ai*, *ti*), where *ai* is the attribute index and *ti* is the threshold value with which *vai* is compared at this node. The same value of *ai* may occur in many nodes, i.e., the same attribute may be evaluated more than once. For each decision node *i*, *L*(*i*) is the index of the next node if $vai \leq ti$; *R*(*i*) is the index of the next node if $vai > ti$. The label nodes are attached with classification information. Repeat the process recursively for p*h*, and so on, until one of the leaf nodes is reached with decision information.

Token Generation:

To generate the private key for the attribute vector v=(*v*1, · · · , *vn*), a client first computes the identity representation set of each element in v and delivers all the *n* identity representation sets to TA. Then TA runs the AnonExtract(id, msk) on each identity id $\in Svi$ in the identity set and delivers all the respective private keys sk*vi* to the client.

Query:

A client delivers the private key sets obtained from the TokenGen algorithm to the cloud, which runs the AnonDecryption algorithm on the ciphertext generated in the Store algorithm. Starting from p1, the decryption result determines which ciphertext should be decrypted next. For instance, if $v1 \in [0, t1]$, then the decryption result indicates the next node index *L*(*i*). The cloud will then use sk*v*(*L*(*i*)) to decrypt the subsequent ciphertext *CL*(*i*). Continue this process iteratively until it reaches a leaf node and decrypt the respective attached information.

Semi Trusted Authority:

A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client input vectors.

ARCHITECTURAL DESIGN:

The major part of the project development sector considers and fully survey all the required needs for developing the project. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations. Generally algorithms shows a result for exploring a single thing that is either be a performance, or speed, or accuracy, and so on. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them.

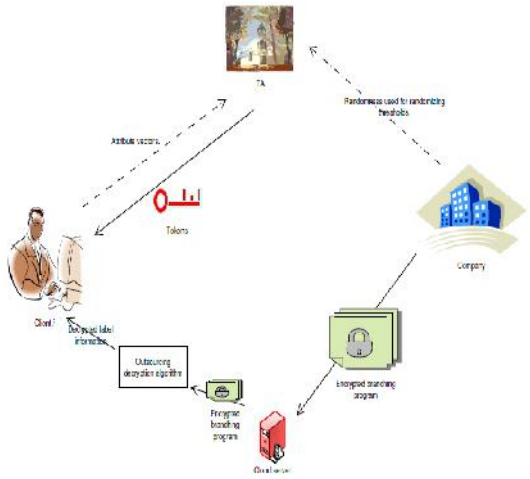


Fig:1. System Architecture

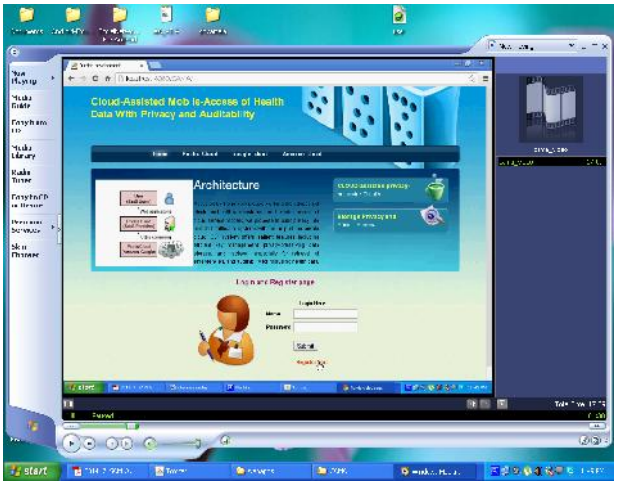
Problem Statement:

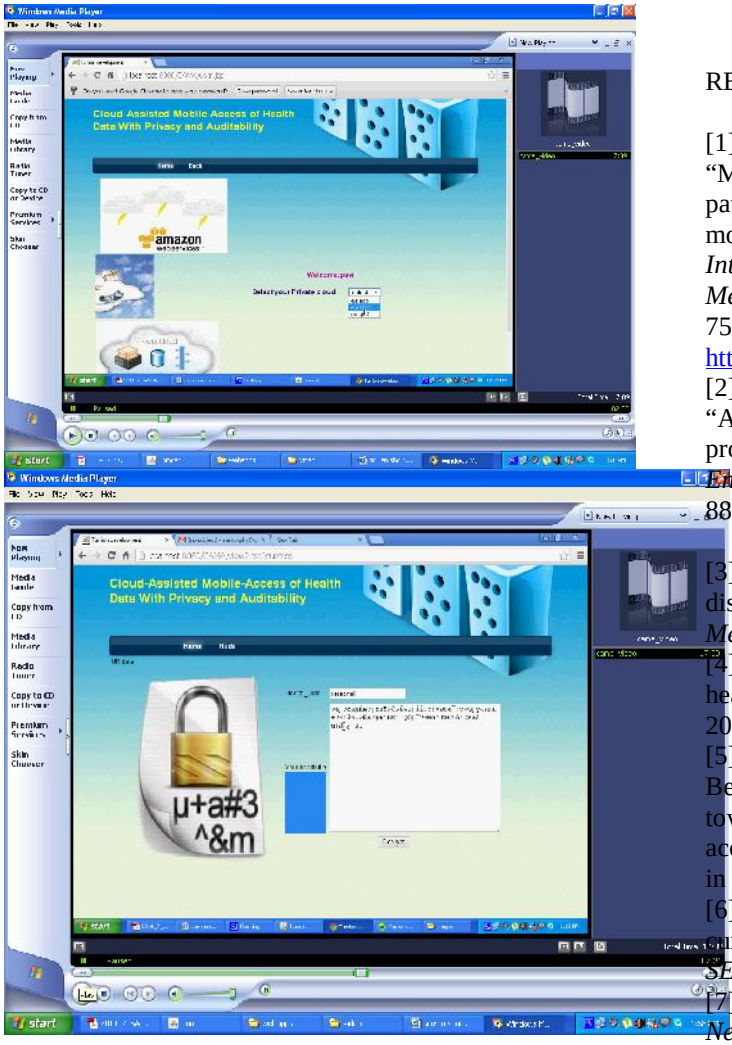
Traditional privacy protection mechanisms by simply removing clients' personal identity information (such as names or SSN) or by using anonymization technique fails to serve as an effective way in dealing with privacy of mHealth systems due to the increasing amount and diversity of personal 2 identifiable information [9]. It is worth noting that the collected information from an mHealth monitoring system could contain clients' personal physical data such as their heights, weights, and blood types, or even their ultimate personal identifiable information such as their fingerprints and DNA profiles. According to, personal identifiable information (PII) is "any information, recorded or otherwise, relating to an identifiable individual. Almost any information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational".

Scope:

CAM consists of four parties: the cloud server (simply the cloud), the company who provides the mHealth monitoring service (i.e., the healthcare service provider), the individual clients (simply clients), and a semi-trusted authority (TA). The company stores its encrypted monitoring data or program in the cloud server. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through a mobile (or smart) device. A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model.

RESULTS:




## CONCLUSION

we design a cloud-assisted privacy preserving mobile health monitoring system, called CAM, which can effectively protect the privacy of clients and the intellectual proerty of mHealth service providers. To protect the clients' privacy, we apply the anonymous Boneh-Franklin identity based encryption (IBE) in medical diagnostic branching programs. To reduce the decryption complexity due to the use of IBE, we apply recently proposed decryption outsourcing with privacy protection to shift clients' pairing computation to the cloud server. To protect mHeath service providers' programs, we expand the branching program tree by using the random permutation and randomize the decision thresholds used at the decision branching nodes. Finally, to enable resource constrained small companies to participate in mHealth business, our CAM design helps them to shift the computational burden to the cloud by applying newly developed key private proxy re-encryption technique. Our CAM has been shown to achieve the design objective.

## REFERENCES

[1] P. Mohan, D. Marin, S. Sultan, and A. Deen, "Medinet: personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony." *Conference Proceedings of the International Conference of IEEE Engineering in Medicine and Biology Society*, vol. 2008, no. 3, pp. 755–758. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/19162765

[2] A. Tsanas, M. Little, P. McSharry, and L. Ramig, "Accurate telemonitoring of parkinson's disease progression by noninvasive speech tests," *Biomedical Engineering, IEEE Transactions on*, vol. 57, no. 4, pp. 884 – 893, 2010.

[3] G. Clifford and D. Clifton, "Wireless technology in disease management and medicine," *Annual Review of Medicine*, vol. 63, pp. 479–492, 2012.

[4] L. Ponemon Institute, "Americans' opinions on healthcare privacy, available: http://tinyurl.com/4atsdlj," 2010.

[5] A. V. Dhukaram, C. Baber, L. Elloumi, B.-J. van Beijnum, and P. D. Stefanis, "End-user perception towards pervasive cardiac healthcare services: Benefits, acceptance, adoption, risks, security, privacy and trust," in *PervasiveHealth*, 2011, pp. 478–484.

[6] M. Delgado, "The evolution of health care it: Are current u.s. privacy policies ready for the clouds?" in *SERVICES*, 2011, pp. 371–378.

[7] N. Singer, "When 2+ 2 equals a privacy question," *New York Times*, 2009.

[8] E. B. Fernandez, "Security in data intensive computing systems," in *Handbook of Data Intensive Computing*, 2011, pp. 447–466.

[9] A. Narayanan and V. Shmatikov, "Myths and fallacies of personally identifiable information," *Communications of the ACM*, vol. 53, no. 6, pp. 24–26, 2010.

[10] P. Baldi, R. Baronio, E. D. Cristofaro, P. Gasti, and G. Tsudik, "Countering gattaca: efficient and secure testing of fully-sequenced human genomes," in *ACM Conference on Computer and Communications Security*, 2011, pp. 691–702.

Sites Referred: